Optics and Lasers in Engineering 101 (2018) 51–59

Contents lists available at ScienceDirect

Optics and Lasers in Engineering

journal homepage: www.elsevier.com/locate/optlaseng

Security enhancement of double random phase encoding using rear-mounted phase masking

Junxin Chen [a,*], Yu Zhang [a], Jinchang Li [a], Li-bo Zhang [b,*]

[a] Sino-Dutch Biomedical and Information Engineering School, Northeastern University, Shenyang 110169, China
[b] Department of Radiology, The General Hospital of Shenyang Command PLA, Shenyang 110016, China

ARTICLE INFO

Keywords:
Double random phase encoding
Security enhancements
Phase masking
Cryptanalysis

ABSTRACT

In this paper, a security enhancement for double random phase encoding (DRPE) by introducing a rear-mounted phase masking procedure is presented. Based on exhaustively studying the cryptanalysis achievements of DRPE and its variants, invalidation of the second lens, which plays a critical role in cryptanalyzing processes, is concluded. The improved system can exploit the security potential of the second lens and consequently strengthen the security of DRPE. Experimental results and security analyses are presented in detail to demonstrate the security potential of the proposed cryptosystem.

1. Introduction

With the increasing number of online image applications, security has become a critical issue in image transmission processes and storage over public networks. Owing to their advantages of high speed and parallel processing, optical systems have drawn significant attraction for fulfilling these increasing security requirements. Refregier and Javidi [1] proposed their pioneering achievement of double random phase encoding (DRPE) and subsequently paved the way for numerous types of optical cryptosystems in the past few decades. In [2], fully phase encoding was introduced to DRPE for providing security enhancement and noise resistance. Various researchers [3–8] have developed optical image cryptosystems by performing DRPE in the fractional Fourier transform domain (FrFT), while *Situ* introduced Fresnel transform (FrT) for DRPE [9]. Some other techniques are also employed to build secure optical cryptosystems; these include the gyrator transform [10], the discrete fractional cosine transform [11,12], the discrete fractional random transform [13,14], phase retrieval [15–17], diffractive imaging [18,19], interference [20,21], photon counting [22], the modified Fourier transform [23], chaotic theory [24,25], random wavefronts [26], and the asymmetric concept [27–31] are.

Recently, cryptanalysis achievements have revealed the vulnerabilities of DRPE to various attacks, such as chosen-ciphertext attack [32], known-plaintext attack [33], and chosen-plaintext attack [34]. The most dangerous attack only requires two known plain images. To further enhance the security of DRPE, improvements in various aspects have been subsequently proposed. To the best of our knowledge, the existing improvements can be classified into six categories. These are (i) using fully phase encoding instead of amplitude encoding [2], (ii) implementing DRPE in different optical transform domains [3–6], (iii) chaos-based random phase mask generation [35], (iv) prepositive pixel randomization using chaos [36], (v) asymmetric design with phase truncation [27], and (vi) amplitude-phase mixing encoding [37]. Unfortunately, these variants have also been successfully cryptanalyzed [38–44]. As DRPE is the simplest and most effective image encryption scheme, how to promote its security level with lower complexity is still an attractive issue.

Given the above, this paper presents a security enhancement for DRPE by introducing a rear-mounted phase masking operation. The contributions can be summarized in three aspects. First, cryptanalysis of DRPE and its variants in six kinds is synthetically and contrastively reviewed, and researchers of optical encryption and security have found representative references to promote their design from the cryptanalysis point of view. Secondly, the most critical part of cryptanalysis is identified: invalidation of the second lens, which is helpful for an adversary for converting the ciphertext into the Fourier domain. This achievement is believed to promote research into exploiting the security aspect of this lens in order to build secure optical encryption schemes. Finally, an improvement of DRPE is proposed by planting an additional phase mask in the output plane. The rear-mounted phase mask will modulate the output of DRPE again, and, in other words, an adversary cannot convert the ciphertext to the Fourier domain without the exact knowledge of this mask. The improved system significantly improves the security contribution of the second lens of DRPE and consequently prevents the comfortable counteraction of this lens. Experimental results are also provided for validation. The rear-mounted phase mask enhancement is

* Corresponding authors.
E-mail addresses: chenjx@bmie.neu.edu.cn (J. Chen), zhanglibo.neu@gmail.com (L.-b. Zhang).

https://doi.org/10.1016/j.optlaseng.2017.09.019
Received 22 June 2017; Received in revised form 21 September 2017; Accepted 21 September 2017
0143-8166/

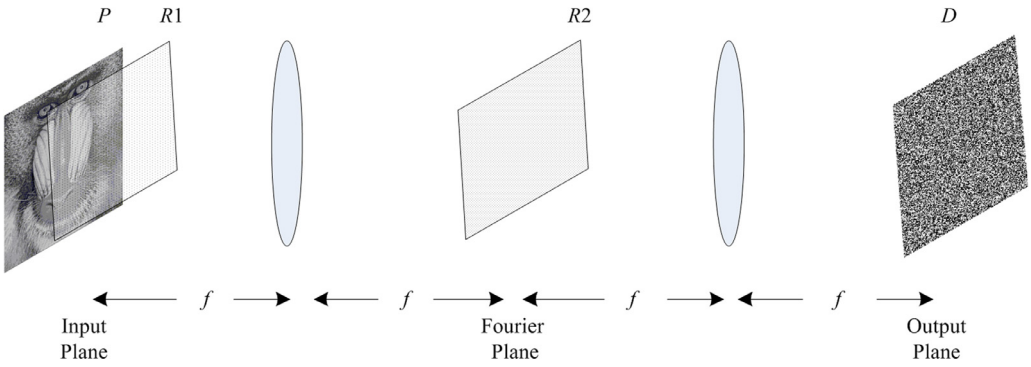

Fig. 1. The 4*f* setup of double random phase encoding.

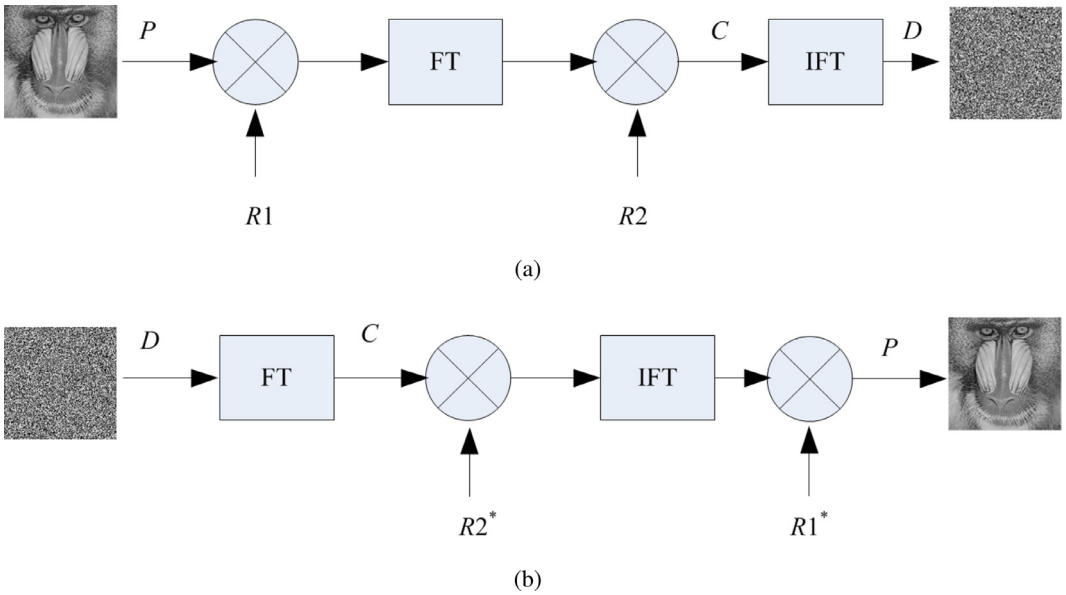

Fig. 2. Flowcharts of DRPE: (a) encryption process; (b) decryption process.

proposed as an exemplary illustration of the security excavation of the second lens, and we hope that interested readers can benefit from the proposed achievements and the other expected enhancements.

The remainder of this paper is organized as follows. DRPE is reviewed in the next section, and its variants and their vulnerabilities are presented in Section 3. In Section 4, the improved scheme is demonstrated in detail, and experimental results are listed in Section 5. Finally, conclusions will be drawn in the last section.

2. DRPE and its cryptanalysis

2.1. DRPE

DRPE is the simplest, most effective, and attractive optical image encryption scheme; a sketch is given in Fig. 1. Following common cryptographic nomenclature, let us denote P as the plain image. The plain image, on which a random phase mask $R1$ is placed, is placed in the input plane of the first lens. In the image focal plane of the first lens, a Fourier transform of $P \cdot R1$ is therefore generated. This product is then immediately point-to-point multiplied by another random phase mask $R2$, and then the result will be converted to the spatial domain by the second lens. In this scheme, the phase masks $R1$ and $R2$ are independently and randomly distributed in $[0, 2\pi]$, and they serve as the secret key of DRPE. The encryption and decryption operations of DRPE can be summarized shown in Figs. 2(a) and (b), respectively, where the superscript * denotes the conjugate of the phase masks. The encrypted image can be written as

$$D = \mathcal{F}^{-1}(R2 \cdot \mathcal{F}(P \cdot R1)), \tag{1}$$

where $\cdot$ denotes point-to-point multiplication, $\mathcal{F}$ represents the two-dimensional Fourier transform, and $\mathcal{F}^{-1}$ is the inverse two-dimensional Fourier transform.

In DRPE, the second lens cannot provide any security contribution and, by knowing the final ciphertext, it is always possible to compute a Fourier transform to offset this operation. Therefore, the cipher image produced in the Fourier domain, as demonstrated in

$$C = R2 \cdot \mathcal{F}(P \cdot R1), \tag{2}$$

is always employed for security analyses.

The decryption process can be simplistically described as

$$P = \mathcal{F}^{-1}(C \div R2) \div R1, \tag{3}$$

in which $\div$ stands for point-to-point division.

2.2. Cryptanalysis of DRPE

In recent years, DRPE has been demonstrated to be vulnerable to various attacks [32–34]. Two classes of attacks have been proposed, one class seeking an exact solution to the random phase masks and another searching for an approximate solution. Among these achievements, the impulse attack in [34] and the phase-retrieval approach in [33] are the most attractive and effective, and these have been further extended to